



Cisco Jabber 14.0 for Windows 10 Security Target

Version: 1.4

Date: August 29, 2022

Cisco Systems, Inc.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

© 2021 Cisco Systems, Inc. All rights reserved.

Table of Contents

| | | |
|-------|--|----|
| 1 | Security Target Introduction..... | 7 |
| 1.1 | ST and TOE Reference | 7 |
| 1.2 | TOE Overview | 7 |
| 1.3 | TOE Product Type | 8 |
| 1.3.1 | Required non-TOE Hardware/Software/Firmware | 8 |
| 1.4 | TOE Description | 8 |
| 1.5 | TOE Evaluated Configuration..... | 9 |
| 1.6 | Physical Scope of the TOE..... | 9 |
| 1.7 | Logical Scope of the TOE | 10 |
| 1.7.1 | Communication..... | 10 |
| 1.7.2 | Cryptographic Support..... | 10 |
| 1.7.3 | User Data protection | 10 |
| 1.7.4 | Identification and Authentication..... | 10 |
| 1.7.5 | Security Management..... | 10 |
| 1.7.6 | Protection of the TSF | 11 |
| 1.7.7 | Trusted Channels | 11 |
| 1.8 | Excluded Functionality..... | 11 |
| 2 | Conformance Claims..... | 12 |
| 2.1 | Common Criteria Conformance Claim | 12 |
| 2.2 | Protection Profile Configuration and Functional Package Conformance Claims | 12 |
| 3 | Security Problem Definition..... | 15 |
| 3.1 | Assumptions | 15 |
| 3.2 | Threats..... | 15 |
| 3.3 | Organizational Security Policies..... | 16 |
| 4 | Security Objectives | 17 |
| 4.1 | Security Objectives for the TOE | 17 |
| 4.2 | Security Objectives for the Environment..... | 19 |
| 4.3 | Security Objectives Rationale | 19 |
| 5 | Security Requirements | 22 |
| 5.1 | Conventions..... | 22 |
| 5.2 | TOE Security Functional Requirements | 22 |
| 5.2.1 | Class: Communications (FCO) | 24 |

- 5.2.1.1 FCO_VOC_EXT.1 – Fixed-Rate Vocoder 24
- 5.2.2 Class: Cryptographic Support (FCS) 24
 - 5.3.2.1 FCS_CKM_EXT.1 – Cryptographic Key Generation Services 24
 - 5.3.2.2 FCS_CKM.1/KeyGen – Cryptographic Asymmetric Key Generation 24
 - 5.3.2.3 FCS_CKM.2 – Cryptographic Key Establishment 25
 - 5.3.2.4 FCS_COP.1/Encrypt – Cryptographic Operation – Encryption/Decryption 25
 - 5.3.2.5 FCS_COP.1/Hash – Cryptographic Operation – Hashing 25
 - 5.3.2.6 FCS_COP.1/SigGen – Cryptographic Operation – Signing 25
 - 5.3.2.7 FCS_COP.1/KeyHash – Cryptographic Operation – Keyed-Hash Message Authentication 26
 - 5.3.2.8 FCS_COP.1/SRTP – Cryptographic Operation – Encryption/Decryption for SRTP 26
 - 5.3.2.9 FCS_RBG_EXT.1 – Random Bit Generation Services..... 26
 - 5.3.2.10 FCS_STO_EXT.1 – Storage of Credentials 26
 - 5.3.2.11 FCS_SRTP_EXT.1 – Secure Real-Time Transport Protocol 26
 - 5.3.2.12 FCS_TLS_EXT.1 – TLS Protocol..... 26
 - 5.3.2.13 FCS_TLSC_EXT.1 – TLS Client Protocol 26
 - 5.3.2.14 FCS_TLSC_EXT.2 – TLS Client Support for Mutual Authentication 27
 - 5.3.2.15 FCS_TLSC_EXT.4 – TLS Client Support for Renegotiation 27
 - 5.3.2.16 FCS_TLSC_EXT.5 – TLS Client Support for Supported Groups Extension 27
- 5.3.3 Class: User Data Protection (FDP) 27
 - 5.3.3.1 FDP_DEC_EXT.1 – Access to Platform Resources..... 27
 - 5.3.3.2 FDP_NET_EXT.1 – Network Communications 27
 - 5.3.3.3 FDP_DAR_EXT.1 – Encryption Of Sensitive Application Data 28
 - 5.3.3.4 FDP_IFC.1 – Subset Information Flow Control 28
 - 5.3.3.5 FDP_IFF.1 – Simple Security Attributes 28
- 5.3.4 Class: Identification and Authentication (FIA) 28
 - 5.3.4.1 FIA_X509_EXT.1 – X.509 Certificate Validation 28
 - 5.3.4.2 FIA_X509_EXT.2 – X.509 Certificate Authentication 29
- 5.3.5 Class: Security Management (FMT) 29
 - 5.3.5.1 FMT_MEC_EXT.1 – Supported Configuration Mechanism 29
 - 5.3.5.2 FMT_CFG_EXT.1 – Secure by Default Configuration 29
 - 5.3.5.3 FMT_SMF.1 – Specification of Management Functions 29
 - 5.3.5.4 FMT_SMF.1/VVoIP – Specification of Management Functions (VVoIP Communications) 29
- 5.3.6 Class: Privacy (FPR) 29
 - 5.3.6.1 FPR_ANO_EXT.1 – User Consent for Transmission of Personally Identifiable Information 29
- 5.3.7 Class: Protection of the TSF (FPT) 30
 - 5.3.7.1 FPT_API_EXT.1 – Use of Supported Services and APIs 30
 - 5.3.7.2 FPT_AEX_EXT.1 – Anti-Exploitation Capabilities 30
 - 5.3.7.3 FPT_TUD_EXT.1 – Integrity for Installation and Update 30
 - 5.3.7.4 FPT_TUD_EXT.2 – Integrity for Installation and Update 30
 - 5.3.7.5 FPT_LIB_EXT.1 – Use of Third Party Libraries..... 30
 - 5.3.7.6 FPT_IDV_EXT.1 Software Identification and Versions..... 32
- 5.3.8 Class: TOE Access (FTA) 32
 - 5.3.8.1 FTA_SSL.3/Media – TSF-Initiated Termination (Media Channel) 32

- 5.3.9 Class: Trusted Path (FTP)..... 32
 - 5.3.9.1 FTP_DIT_EXT.1 – Protection of Data in Transit 32
 - 5.3.9.2 FTP_ITC.1/Control – Inter-TSF Trusted Channel (Signaling Channel) 32
 - 5.3.9.3 FTP_ITC.1/Media – Inter-TSF Trusted Channel (Media Channel) 32
- 5.4 Security Assurance Requirements 32
 - 5.4.1 SAR Requirements 32
 - 5.4.2 SAR Rationale..... 33
- 5.5 Assurance Measures..... 33
- 6 TOE Summary Specification 35
 - 6.1 TOE Security Functional Requirement Measures 35
- 7 Supplemental TOE Summary Specification Information..... 42
- 8 Annex A: References..... 43
- 9 Annex B: Acronyms..... 44
- 10 Annex C: Terminology..... 46
- 11 Annex D: Differing SFR Naming Conventions..... 47
- 12 Annex E: Obtaining Documentation and Submitting a Service Request 48

Table of Tables

- Table 1. ST and TOE Identification..... 7
- Table 2. IT Environment Component..... 8
- Table 3. Excluded Functionality and Rationale 11
- Table 4. PP Configuration and Functional Package Conformance Claims 12
- Table 5. NIAP Technical Decisions Applied to This ST..... 12
- Table 6. TOE Assumptions 15
- Table 7. Threats..... 16
- Table 8. Security Objectives for the TOE 17
- Table 9. Security Objectives for the Environment 19
- Table 10. Security Objectives Rationale 19
- Table 11. Security Requirement Conventions 22
- Table 12. Security Functional Requirements 22
- Table 13. Third-Party Libraries 30
- Table 14. SAR Requirements 33
- Table 15. Assurance Measures 33
- Table 16. How TOE SFRs Measures Are Met 35
- Table 17. CAVP Certificates 42
- Table 18. References 43
- Table 19. Acronyms 44
- Table 20. Terms 46
- Table 21. SFR Naming Map..... 47

Table of Figures

Figure 1. TOE in Relation to the IT Environment 9

Document Introduction

Prepared By:
 Cisco Systems, Inc.
 170 West Tasman Dr.
 San Jose, CA 95134

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), Cisco Jabber 14.0 for Windows 10 (Jabber for Windows 10). This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE that meet the set of requirements. Administrators of the TOE will be referred to as administrators, Authorized Administrators, TOE administrators, semi-privileged administrators, privileged administrators, and security administrators in this document.

Revision History

| Version | Date | Change |
|---------|-------------------|--|
| 0.1 | March 11, 2021 | Initial Version |
| 0.2 | May 28, 2021 | Response to Lab Comments |
| 0.3 | June 4, 2021 | Response to Lab Comments |
| 0.4 | August 16, 2021 | Response to Lab Comments |
| 0.5 | August 30, 2021 | Response to Lab Comments |
| 0.6 | September 7, 2021 | TD Update |
| 0.7 | December 1, 2021 | Response to NIAP |
| 0.8 | February 8, 2022 | Claims Modification |
| 0.9 | March 2, 2022 | Response to Validator Comments |
| 1.0 | July 7, 2022 | Response to Validator Comments and Claims Modification |
| 1.1 | July 15, 2022 | Response to Lab Comments |
| 1.2 | August 2, 2022 | Response to Validator Comments |
| 1.3 | August 17, 2022 | Response to Validator Comments |
| 1.4 | August 29, 2022 | Response to Validator Comments |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2021 Cisco Systems, Inc. All rights reserved.

1 Security Target Introduction

This Security Target contains the following sections:

- Security Target Introduction [Section 1]
- Conformance Claims [Section 2]
- Security Problem Definition [Section 3]
- Security Objectives [Section 4]
- Security Requirements [Section 5]
- TOE Summary Specification [Section 6]
- Supplemental TOE Summary Specification Information [Section 7]
- References

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 3, Chapter 4.

1.1 ST and TOE Reference

This section provides information needed to identify and control this ST and its TOE.

Table 1. ST and TOE Identification

| Name | Description |
|----------------------|--|
| ST Title | Cisco Jabber 14.0 for Windows 10 Security Target |
| ST Version | 1.4 |
| Publication Date | 29 August 2022 |
| Vendor and ST Author | Cisco Systems, Inc. |
| TOE Reference | Cisco Jabber 14.0 for Windows 10 |
| TOE Software Version | 14.0 |
| Keywords | VVoIP Client, Telephony |

1.2 TOE Overview

Cisco Jabber provides users within an organization a number of features for collaborative communication:

Integrated Voice and Video Telephony - Securely make, receive, and control phone calls. Users have a variety of call control options including mute, call transfer, call forwarding, and impromptu conferencing.

Instant Messaging and Presence - View real-time availability of co-workers and securely chat in real time using instant messaging to save time and reduce phone tag.

Online Web Conferencing – Securely access online web conferencing services to collaborate in real-time.

Voicemail Services – Securely access voicemail and tools for managing messages.

The Common Criteria evaluation was limited to the Integrated Voice and Video over IP (VVVoIP) telephony features of Cisco Jabber that it secures with SRTP and TLS 1.2. Video, Instant Messaging and Presence, Online Web Conferencing, and Voicemail Services is not covered by the evaluation. Additionally, call control options other than call placement and call receipt were not evaluated. Advanced features such as call transfer, call forwarding, and impromptu conferencing make use of SIP TLS 1.2, which is part of the evaluation.

1.3 TOE Product Type

The TOE is a software application that provides protected channels for interactive communication. Use case 3 (Communication) as described in [App], use case 2 (Software Application) as described in [VVVoIP], and use case 3 (Client-Server Architecture) in [VVVoIP] apply to the TOE.

1.3.1 Required non-TOE Hardware/Software/Firmware

The TOE has required environmental components to allow for operation and evaluation. The table below lists required IT environment components.

Table 2. IT Environment Component

| Component | Required | Usage/Purpose Description for TOE performance |
|-------------------------------|----------|---|
| Windows 10 Platform | Yes | The TOE requires a Windows 10 OS platform. |
| Enterprise Session Controller | Yes | The Cisco Unified Communications Manager (CUCM) is the SIP Server that provides the TOE with call control and management. CUCM also acts as the configuration server. |
| Remote VoIP Application | Yes | This is the peer VoIP Application that the TOE interacts with using Security Real Time Transport Protocol (SRTP). |
| Certificate Authority | Yes | The Certification Authority provides X.509 certificates. The CA also provides a method to check the certificate revocation status of the CUCM Server. |

1.4 TOE Description

Cisco Jabber allows users of an organization to securely make, receive, and control phone calls through Cisco Unified Communications Manager (CUCM). Users have a variety of call-control options including mute, call transfer, call forwarding, and impromptu conferencing. Figure 1 depicts the TOE in relation to the IT environment.

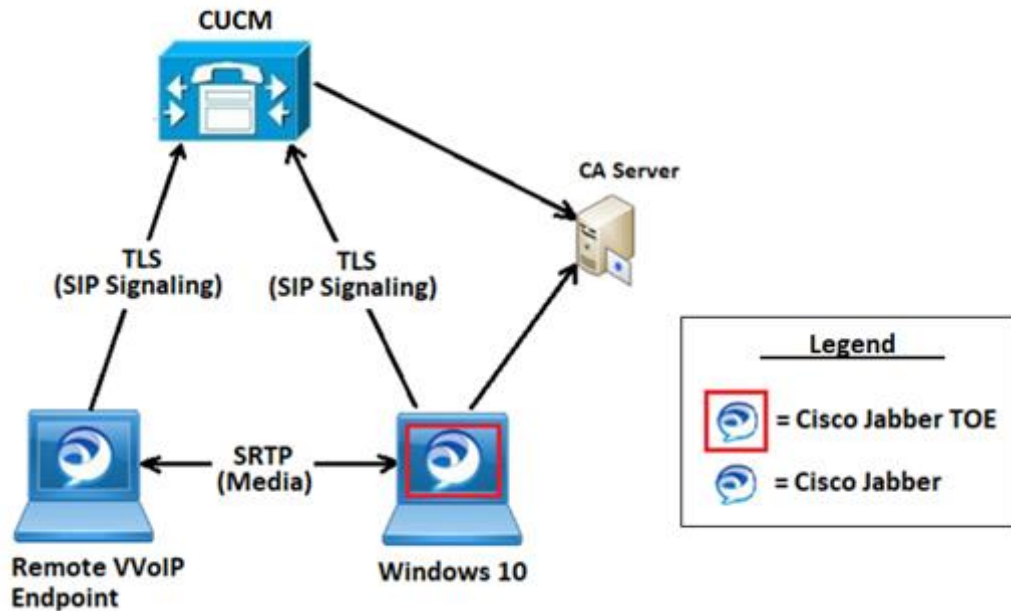


Figure 1. TOE in Relation to the IT Environment

Note: In the test environment, only one instance of Jabber is considered the TOE (outlined in red above). The TOE is limited by the Protection Profile regarding what TLS version and ciphers may be claimed. However, the TOE only exchanges SIP messaging with the ESC (CUCM), and there is nothing requiring other endpoints use TLS 1.2 exclusively, so for non-TOE endpoints, there is no limitation placed on the TLS version.

1.5 TOE Evaluated Configuration

The evaluated configuration is a single instance of Cisco Jabber operating in FIPS and CC mode. Refer to the Cisco Jabber for Windows 10 Common Criteria Configuration Guide for instructions on placing Cisco Jabber in FIPS and CC mode.

CUCM, release 12.0 or later, is the ESC (also referred to as the SIP Server) that serves as the call control component for voice and video. There are configuration settings the CUCM ‘pushes’ to the Cisco Jabber TOE, a form of management permitted in [VVoIP].

CUCM is required to be configured in the On-Premises deployment mode for softphones. Refer to the Cisco Jabber for Windows 10 Common Criteria Configuration Guide for specific information regarding configuring CUCM in the On-Premises deployment mode for softphones.

The specific software version evaluated was 14.0.1 and 14.0.4. The version 14.0.4 was used to complete the evaluation of the Assurance Activities related to the following SFRs: FCS_SRTP_EXT.1, FIA_X509_EXT.1, FDP_IFF.1, FPT_IDV_EXT.1, FPT_TUD_EXT.1.

NOTE: Version 14.0.4 did not impact SFRs that were already tested. Version 14.0.4 allowed the TOE to meet the SFR listed above.

1.6 Physical Scope of the TOE

The TOE is a software-only client application that executes on a Windows 10 platform.

1.7 Logical Scope of the TOE

The TOE is comprised of several security features. Each of the security features consists of several security functionalities, as identified below.

- Communication
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Trusted Channels

These features are described in more detail in the subsections below.

1.7.1 Communication

The Cisco Jabber TOE transmits voice media using a constant bitrate (CBR) vocoder.

1.7.2 Cryptographic Support

The Cisco Jabber TOE provides cryptography in support of SIP connections via Security Real-Time Transport Protocol (SRTP) established using the Session Description Protocol (SDP) and the Security Descriptions for Media Streams (SDS) for SDP. The TOE also protects communications between itself and the CUCM SIP Server by using a Transport Layer Security (TLS)-protected signaling channel.

The TOE incorporates a CiscoSSL cryptographic module library (v7.2), and the algorithm implementation has been validated for CAVP conformance. See Table 17 in Section 7 for certificate references.

1.7.3 User Data protection

The TOE ensures that user data is not transmitted when a call is placed on hold, a call is placed on mute, or when the TOE is not registered with the SIP server. Additionally, the TOE restricts access to hardware resources and network communications to only those required.

1.7.4 Identification and Authentication

The TOE performs X.509 certificate authentication of remote components the TOE interacts with for SDS/SRTP and TLS connections. The Cisco Jabber TOE relies upon the TOE Platform to validate certificates.

1.7.5 Security Management

The TOE is capable of registering with an Enterprise Session Controller (ESC) and specifying the termination period for idle calls.

1.7.6 Protection of the TSF

The TOE leverages services and APIs provided by the platform in order to support anti-exploitation features and installation of authorized software updates.

1.7.7 Trusted Channels

The TOE’s implementation of SDES-SRTP allows secure voice and video communication between itself and a remote VVoIP application and secure signaling communication between itself and a remote CUCM SIP Server using TLS.

1.8 Excluded Functionality

The following functionality is not included in the CC evaluation:

Table 3. Excluded Functionality and Rationale

| Function Excluded | Rationale |
|--|---|
| Non-FIPS 140-2 and non-CC modes of operation | FIPS and CC modes of operation must be enabled in order for the TOE to be operating in its evaluated configuration. |
| SRTP with NULL cipher | SRTP with the NULL cipher does not provide encryption. |
| Jabber to Jabber calling. Jabber to Jabber calling provides basic voice and video calling capabilities between different Cisco Jabber clients without registering to Cisco Unified Communications Manager. | This feature is not TSF relevant functionality included in the Protection Profiles. |
| Cisco Instant Message and Presence Service (Instant Messaging and Presence) | This feature is not TSF relevant functionality included in the Protection Profiles. |
| Cisco Webex® Meetings Server (Online Web Conferencing) | This feature is not TSF relevant functionality included in the Protection Profiles. |
| Cisco Unity® Connection (Voicemail) | This feature is not TSF relevant functionality included in the Protection Profiles. |
| IBM Lotus Notes and Google Calendar | This feature is not TSF relevant functionality included in the Protection Profiles. |

The functionality listed above is disabled in the TOE evaluated configuration.

2 Conformance Claims

2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 5, dated: September 2012. For a listing of Assurance Requirements claimed see Section 5.4.

The TOE and ST are CC Part 2 extended and CC Part 3 extended conformant.

2.2 Protection Profile Configuration and Functional Package Conformance Claims

The TOE and ST are conformant with the Specifications listed in the table below:

Table 4. PP Configuration and Functional Package Conformance Claims

| Specification | Version | Date | Short Name |
|---|---------|------------|--------------------|
| PP-Configuration for Application Software and Voice/Video over IP (VVoIP) Endpoints | V1.0 | 2020-10-28 | CFG_APP-VVOIP_v1.0 |
| The PP-Configuration includes the following components: | | | |
| <ul style="list-style-type: none"> Protection Profile for Application Software | V1.3 | 2019-03-01 | PP_APP_v1.3 |
| <ul style="list-style-type: none"> PP-Module for Voice and Video over IP (VVoIP) | V1.0 | 2020-10-28 | MOD_VVOIP_V1.0 |
| Package Claim: | | | |
| Functional Package for TLS | V1.1 | 2019-03-01 | PKG_TLS_V1.1 |

The following NIAP Technical Decisions (TD) have also been applied to the claims in this document. Each posted TD was reviewed and considered based on the TOE product type, the PP claims, and the security functional requirements claimed in this document.

Table 5. NIAP Technical Decisions Applied to This ST

| TD Identifier | TD Name | Protection Profiles | References | Publication Date | Applicable? |
|---------------|---|--|---|------------------|---|
| TD0601 | X.509 SFR Applicability in App PP | PP_APP_v1.3 | FIA_X509_EXT.1, FIA_X509_EXT.2, FTP_DIT_EXT.1, FCS_HTTPS_EXT.1 | 2021.09.22 | Yes - TD has been applied |
| TD0600 | Conformance claim sections updated to allow for MOD_VPNC_V2.3 | MOD_BT_V1.0, MOD_FE_V1.0, MOD_FEEM_V1.0, MOD_MDM_AGENT_V1.0, PP_APP_v1.3, PP_MDF_V3.2, PP_MDM_V4.0, PP_OS_V4.2.1 | Section 2 | 2021.08.10 | No – No claims related to MOD_VPNC_V2.3 |

| TD Identifier | TD Name | Protection Profiles | References | Publication Date | Applicable? |
|---------------|---|---------------------|---------------------------------|------------------|--------------------------------|
| TD0589 | Reliable Time for VVoIP Software TOEs | MOD_VVOIP_V1.0 | FPT_STM_EXT.1/VVoIP | 2021.05.14 | Yes - TD has been applied |
| TD0588 | Session Resumption Support in TLS package | PKG_TLS_V1.1 | FCS_DTLSS_EXT.1, FCS_TLSS_EXT.1 | 2021.05.12 | No – No TLS Server claims |
| TD0598 | Expanded AES Modes in FCS_COP for App PP | PP_APP_V1.3 | FCS_COP.1/Encrypt | 2021.08.03 | Yes - TD has been applied |
| TD0582 | PP-Configuration for Application Software and Virtual Private Network (VPN) Clients now allowed | PP_APP_v1.3 | Section 2, FDP_DAR_EXT.1 | 2021.04.16 | Yes - TD has been applied |
| TD0561 | Signature verification update | PP_APP_v1.3 | FPT_TUD_EXT.1.4, FPT_TUD_EXT.2 | 2021.01.15 | Yes - TD has been applied |
| TD0554 | OS/iPadOS/Android AppSW Virus Scan | PP_APP_v1.3 | AVA_VAN.1 | 2020.10.30 | Yes - TD has been applied |
| TD0548 | Integrity for installation tests in AppSW PP 1.3 | PP_APP_v1.3 | FPT_TUD_EXT.1.3 | 2020.09.30 | Yes - TD has been applied |
| TD0544 | Alternative testing methods for FPT_AEX_EXT.1.1 | PP_APP_v1.3 | FPT_AEX_EXT.1 | 2020.09.15 | Yes - TD has been applied |
| TD0543 | FMT_MEC_EXT.1 evaluation activity update | PP_APP_v1.3 | FMT_MEC_EXT.1 | 2020.09.15 | Yes - TD has been applied |
| TD0519 | Linux symbolic links and FMT_CFG_EXT.1 | PP_APP_v1.3 | FMT_CFG_EXT.1.2 | 2020.06.18 | No – Not a Linux Platform |
| TD0515 | Use Android APK manifest in test | PP_APP_v1.3 | FDP_DEC_EXT.1 | 2020.06.08 | No – Not an Android Platform |
| TD0513 | CA Certificate loading | PKG_TLS_V1.1 | FCS_TLSC_EXT.1.3 | 2020.05.26 | Yes - TD has been applied |
| TD0510 | Obtaining random bytes for iOS/macOS | PP_APP_v1.3 | FCS_RBG_EXT.1 | 2020.03.03 | No – Not an iOS/macOS Platform |
| TD0499 | Testing with pinned certificates | PKG_TLS_V1.1 | FCS_TLSC_EXT.1.2 | 2020.02.04 | Yes - TD has been applied |
| TD0498 | Application Software PP Security Objectives and Requirements Rationale | PP_APP_v1.3 | Section 4.3 and Section 5.2 | 2020.01.31 | Yes - TD has been applied |
| TD0495 | FIA_X509_EXT.1.2 Test Clarification | PP_APP_v1.3 | FIA_X509_EXT.1.2 | 2020.01.29 | Yes - TD has been applied |
| TD0469 | Modification of test activity for FCS_TLSS_EXT.1.1 test 4.1 | PKG_TLS_V1.1 | FCS_TLSS_EXT.1.1 | 2019.11.20 | No – No TLS Server claims |
| TD0465 | Configuration Storage for .NET Apps | PP_APP_v1.3 | FMT_MEC_EXT.1 | 2019.11.08 | Yes - TD has been applied |
| TD0445 | User Modifiable File Definition | PP_APP_v1.3 | FPT_AEX_EXT.1.4 | 2019.10.09 | Yes - TD has been applied |

| TD Identifier | TD Name | Protection Profiles | References | Publication Date | Applicable? |
|---------------|--|-----------------------------|---|------------------|---------------------------|
| TD0442 | Updated TLS Ciphersuites for TLS Package | PKG_TLS_V1.1 | FCS_TLSC_EXT.1.1, FCS_TLSS_EXT.1.1, FCS_DTLSC_EXT.1.1, FCS_DTLSS_EXT.1.1 | 2019.08.21 | Yes - TD has been applied |
| TD0437 | Supported Configuration Mechanism | PP_APP_v1.3 | FMT_MEC_EXT.1.1 | 2019.07.23 | Yes - TD has been applied |
| TD0435 | Alternative to SELinux for FPT_AEX_EXT.1.3 | PP_APP_v1.2, PP_APP_v1.3 | FPT_AEX_EXT.1.3 | 2019.07.26 | No – Not a Linux Platform |
| TD0434 | Windows Desktop Applications Test | PP_APP_v1.2, PP_APP_v1.3 | FDP_DEC_EXT.1.1 | 2019.07.22 | Yes - TD has been applied |
| TD0427 | Reliable Time Source | PP_APP_v1.2, PP_APP_v1.3 | A.Platform | 2019.06.11 | Yes - TD has been applied |
| TD0416 | Correction to FCS_RBG_EXT.1 Test Activity | PP_APP_v1.3 | FCS_RBG_EXT.1.1 | 2019.04.24 | Yes - TD has been applied |

3 Security Problem Definition

This section identifies the following:

- Significant assumptions about the TOE’s operational environment
- IT related threats to the organization countered by the TOE
- Environmental threats requiring controls to provide sufficient protection
- Organizational Security Policies for the TOE as appropriate

This document identifies assumptions as A.assumption with “assumption” specifying a unique name. Threats are identified as T.threat with “threat” specifying a unique name. Organizational Security Policies (OSPs) are identified as P.osp with “osp” specifying a unique name.

3.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE’s environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 6. TOE Assumptions

| Assumption | Assumption Definition |
|-----------------|---|
| A.PLATFORM | The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE. |
| A.PROPER_USER | The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy. |
| A.PROPER_ADMIN | The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy. |
| A.UPDATE_SOURCE | It is assumed that TOE software/firmware updates will be made available on either the call control server that the TOE connects to or a separate file server managed by the organization. |

3.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Table 7. Threats

| Threat | Threat Definition |
|---------------------------|--|
| T.NETWORK_ATTACK | An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it. |
| T.NETWORK_EAVESDROP | An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints. |
| T.LOCAL_ATTACK | An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications. |
| T.PHYSICAL_ACCESS | An attacker may try to access sensitive data at rest. |
| T.MEDIA_DISCLOSURE | An attacker can use the encrypted variable rate vocoder frames to their advantage to decode transmitted data. |
| T.UNDETECTED_TRANSMISSION | An attacker may cause the TOE to exfiltrate audio or video media over a remote channel while in a state where the user has a reasonable expectation that no media is being transmitted. |

3.3 Organizational Security Policies

There are no organizational security policies defined in [App], [VVoIP], or [TLS]

4 Security Objectives

This section identifies the security objectives of the TOE and the IT Environment. The security objectives identify the responsibilities of the TOE and the TOE’s IT environment in meeting the security needs.

This document identifies objectives of the TOE as O.objective with “objective” specifying a unique name. Objectives that apply to the IT environment are designated as OE.objective with “objective” specifying a unique name.

4.1 Security Objectives for the TOE

The following table, Security Objectives for the TOE, identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified. An explanation of the relationship between the objectives and the threats/policies is provided in the rationale section of this document.

Table 8. Security Objectives for the TOE

| Environment Security Objective | IT Environment Security Objective Definition | Addressed By |
|--------------------------------|--|--|
| O.INTEGRITY | Conformant TOEs ensure the integrity of their installation and update packages, and also leverage execution environment-based mitigations. Software is seldom, if ever, shipped without errors. The ability to deploy patches and updates to fielded software with integrity is critical to enterprise network security. Processor manufacturers, compiler developers, execution environment vendors, and operating system vendors have developed execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. Application software can often take advantage of these mechanisms by using APIs provided by the runtime environment or by enabling the mechanism through compiler or linker options. | FDP_DEC_EXT.1, FMT_CFG_EXT.1, FPT_AEX_EXT.1, FPT_TUD_EXT.1, FCS_RBG_EXT.1 |
| O.QUALITY | To ensure quality of implementation, conformant TOEs leverage services and APIs provided by the runtime environment rather than implementing their own versions of these services and APIs. This is especially important for cryptographic services and other complex operations such as file and media parsing. Leveraging this platform behavior relies upon using only documented and supported APIs. | FMT_MEC_EXT.1, FPT_API_EXT.1, FPT_API_EXT.2, FPT_LIB_EXT.1, FPT_TUD_EXT.2, FCS_CKM.1/KeyGen, FCS_RBG_EXT.1, FCS_CKM_EXT.1, FCS_STO_EXT.1, FDP_DAR_EXT.1, FCS_CKM.2, FIA_X509_EXT.1 |
| O.MANAGEMENT | To facilitate management by users and the enterprise, conformant TOEs provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration. This also includes providing control to the user regarding disclosure of any PII. | FMT_SMF.1, FPT_IDV_EXT.1, FPT_TUD_EXT.1, FPR_ANO_EXT.1, FCS_COP.1/SigGen |

| Environment Security Objective | IT Environment Security Objective Definition | Addressed By |
|--------------------------------|--|--|
| O.PROTECTED_STORAGE | To address the issue of loss of confidentiality of user data in the event of loss of physical control of the storage medium, conformant TOEs will use data-at-rest protection. This involves encrypting data and keys stored by the TOE in order to prevent unauthorized access to this data. This also includes unnecessary network communications whose consequence may be the loss of data. | FDP_DAR_EXT.1, FCS_STO_EXT.1, FCS_RBG_EXT.1, FCS_CKM.1/Password, FCS_COP.1/Encrypt, FCS_COP.1/Hash, FCS_COP.1/KeyHash |
| O.PROTECTED_COMMS | To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant TOEs will use a trusted channel for sensitive data. Sensitive data includes cryptographic keys, passwords, and any other data specific to the application that should not be exposed outside of the application. | FTP_DIT_EXT.1, FCS_RBG_EXT.1, FCS_RBG_EXT.2, FCS_CKM_EXT.1, FCS_CKM.2, FDP_NET_EXT.1, FIA_X509_EXT.1, FCS_CKM.1/KeyGen, FCS_COP.1/Encrypt, FCS_COP.1/Hash, FCS_COP.1/SigGen, FCS_COP.1/KeyHash, FIA_X509_EXT.2 |
| O.ENCRYPTION | To prevent data disclosure from decryption, conformant TOEs will transmit and store sensitive data using mechanisms that provide adequate protections. | FCS_NTP_EXT.1 (from NDcPP), FCS_TLSC_EXT.1 (refined from NDcPP), FCS_TLSC_EXT.2 (refined from NDcPP), FIA_X509_EXT.1/Rev (refined from NDcPP), FIA_X509_EXT.2 (refined from NDcPP), FIA_X509_EXT.3 (refined from NDcPP), FTP_ITC.1 (refined from NDcPP), FTP_DIT_EXT.1 (refined from App PP), FCO_VOC_EXT.1, FTP_ITC.1/Control, FTP_ITC.1/Media, FAU_STG_EXT.1 (optional for software-only TOEs), FCS_COP.1/SRTP (selection-based), FCS_SRTP_EXT.1 (selection-based), FDP_IFC.1/CallControl (selection-based), FDP_IFF.1/CallControl (selection-based), FPT_STM_EXT.1/VVoIP (selection-based), FCS_TLS_EXT.1.1 |
| O.NO_UNATTENDED_TRANSMISSION | To prevent undetected transmissions, conformant TOEs will not transmit unattended voice or video data when streaming media is not in use. | FDP_IFC.1, FDP_IFF.1, FTA_SSL.3/Media, FAU_GEN.1/CS-Admin (optional), FAU_GEN.1/CS-VVoIP (optional), FAU_GEN.1/P2P-Admin (selection-based), FAU_GEN.1/P2P-VVoIP (selection-based), FPT_STM_EXT.1/VVoIP (selection-based) |

| Environment Security Objective | IT Environment Security Objective Definition | Addressed By |
|--------------------------------|---|-----------------|
| O.TOE_ADMINISTRATION | To support the enforcement of other security functionality, a conformant TOE will provide a management capability that allows for configuration of the TSF. | FMT_SMF.1/VVoIP |

4.2 Security Objectives for the Environment

All of the assumptions stated in Section 3.1 are considered to be security objectives for the environment. The following are the non-IT security objectives, which, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 9. Security Objectives for the Environment

| Environment Security Objective | IT Environment Security Objective Definition |
|--------------------------------|--|
| OE.PLATFORM | The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE. |
| OE.PROPER_USER | The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy. |
| OE.PROPER_ADMIN | The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy. |
| OE.UPDATE_SOURCE | The operational environment will have TOE software/firmware made available on either the call control server that the TOE connects to or a separate file server managed by the organization. |

4.3 Security Objectives Rationale

This section describes how the assumptions, threats, and organizational security policies map to the security objectives.

Table 10. Security Objectives Rationale

| Threats, Assumptions, or Policy | Security Objective | Rationale |
|--|--------------------|---|
| T.NETWORK_ATTACK An attacker is positioned on a communications channel or | O.PROTECTED_COMMS | The threat T.NETWORK_ATTACK is countered by O.PROTECTED_COMMS as this provides for integrity of transmitted data. |

| Threats, Assumptions, or Policy | Security Objective | Rationale |
|---|---------------------|---|
| elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it. | O.INTEGRITY | The threat T.NETWORK_ATTACK is countered by O.INTEGRITY as this provides for integrity of software that is installed onto the system from the network. |
| | O.MANAGEMENT | The threat T.NETWORK_ATTACK is countered by O.MANAGEMENT as this provides for the ability to configure the application to defend against network attack. |
| T.NETWORK_EAVESDROP An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints. | O.PROTECTED_COMMS | The threat T.NETWORK_EAVESDROP is countered by O.PROTECTED_COMMS as this provides for confidentiality of transmitted data. |
| | O.QUALITY | The objective O.QUALITY ensures use of mechanisms that provide protection against network-based attack. |
| | O.MANAGEMENT | The threat T.NETWORK_EAVESDROP is countered by O.MANAGEMENT as this provides for the ability to configure the application to protect the confidentiality of its transmitted data. |
| T.LOCAL_ATTACK An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications. | O.QUALITY | The objective O.QUALITY protects against the use of mechanisms that weaken the TOE with regard to attack by other software on the platform. |
| T.PHYSICAL_ACCESS An attacker may try to access sensitive data at rest. | O.PROTECTED_STORAGE | The objective O.PROTECTED_STORAGE protects against unauthorized attempts to access physical storage used by the TOE. |
| A.PLATFORM | OE.PLATFORM | The operational environment objective OE.PLATFORM is realized through A.PLATFORM. |
| A.PROPER_USER | OE.PROPER_USER | The operational environment Objective OE.PROPER_USER is realized through A.PROPER_USER. |
| A.PROPER_ADMIN | OE.PROPER_ADMIN | The operational environment Objective OE.PROPER_ADMIN is realized through A.PROPER_ADMIN. |

| Threats, Assumptions, or Policy | Security Objective | Rationale |
|---------------------------------|------------------------------|--|
| T.MEDIA_DISCLOSURE | O.ENCRYPTION | The TOE transmits security-relevant data to environmental IT entities using cryptographic mechanisms that protect this data from unauthorized disclosure. |
| T.UNDETECTED_TRANSMISSION | O.NO_UNATTENDED_TRANSMISSION | The TOE prevents transmission of all unattended voice or video data when the streaming media is not in use, thereby ensuring that data is only transmitted when affirmatively directed by the user. Auditing (optional for software only TOE's) further assists in detecting transmission of VVOIP data. |
| | O.TOE_ADMINISTRATION | The TOE defines management functions for VVoIP connectivity and optionally allows for configuration of the idle period for calls to minimize the risk of active unattended sessions and configuration of auditing to specify how transmissions are recorded. |
| A.UPDATE_SOURCE | OE.UPDATE_SOURCE | The objective satisfies the assumption by ensuring that TOE updates are made available in the intended location. |

5 Security Requirements

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, dated: April 2017 and all international interpretations.

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements in this section are derived from [APP], [VVoIP], [TLS], and NIAP TDs.

5.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

Table 11. Security Requirement Conventions

| Convention | Indication |
|-----------------------|--|
| Assignment | Indicated with italicized text (e.g., <i>assignment</i>). |
| Selection | Indicated with underlined text; (e.g., <u>selection</u>). |
| Iteration | Indicated by appending the SFR name with a slash and unique identifier suggesting the purpose of the iteration. (e.g. "FCS_COP.1/Hash"). |
| Refinement | Indicated with bold text and strikethroughs. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "... all objects ..." or "... some big things ..."). |
| Extended Requirements | Are identified with "(_EXT)" in of the functional class/name and are those not found in Part 2 of the CC. |
| Other | Sections of the ST use bolding to highlight text of special interest, such as captions. |

Note that iterations in [App] are identified with a number inside parentheses (e.g. "(1)") and iterations in [VVoIP] are identified by appending the SFR name with a slash and unique identifier suggesting the purpose of the iteration. This ST will follow the convention defined in [VVoIP] for iteration. For clarity, a mapping between the two formats, for SFRs related to this ST, has been included in Annex D: Differing SFR Naming Conventions.

5.2 TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear in the following table are described in more detail in the following subsections.

Table 12. Security Functional Requirements

| Class Name | Component Identification | Component Name | Drawn From |
|----------------------------|--------------------------|---------------------------------------|------------|
| FCO: Communications | FCO_VOC_EXT.1 | Fixed-Rate Vocoder | [VVoIP] |
| FCS: Cryptographic support | FCS_CKM_EXT.1 | Cryptographic Key Generation Services | [APP] |

| Class Name | Component Identification | Component Name | Drawn From |
|---|--------------------------|---|---------------|
| | FCS_CKM.1/KeyGen | Cryptographic Asymmetric Key Generation | [APP] |
| | FCS_CKM.2 | Cryptographic Key Establishment | [APP] |
| | FCS_COP.1/Encrypt | Cryptographic Operation – Encryption/Decryption | [APP] |
| | FCS_COP.1/Hash | Cryptographic Operation – Hashing | [APP] |
| | FCS_COP.1/SigGen | Cryptographic Operation – Signing | [APP] |
| | FCS_COP.1/KeyHash | Cryptographic Operation – Keyed–Hash Message Authentication | [APP] |
| | FCS_COP.1/SRTP | Cryptographic Operation – Encryption/Decryption for SRTP | [VVoIP] |
| | FCS_RBG_EXT.1 | Random Bit Generation Services | [APP] |
| | FCS_STO_EXT.1 | Storage of Credentials | [APP] |
| | FCS_SRTP_EXT.1 | Secure Real-Time Transport Protocol | [VVoIP] |
| | FCS_TLS_EXT.1 | TLS Protocol | [TLS] |
| | FCS_TLSC_EXT.1 | TLS Client Protocol | [TLS] [VVoIP] |
| | FCS_TLSC_EXT.2 | TLS Client Support for Mutual Authentication | [TLS] [VVoIP] |
| | FCS_TLSC_EXT.4 | TLS Client Support for Renegotiation | [TLS] |
| | FCS_TLSC_EXT.5 | TLS Client Support for Supported Groups Extension | [TLS] |
| FDP: User Data Protection | FDP_DEC_EXT.1 | Access to Platform Resources | [APP] |
| | FDP_NET_EXT.1 | Network Communications | [APP] |
| | FDP_DAR_EXT.1 | Encryption Of Sensitive Application Data | [APP] |
| | FDP_IFC.1 | Subset Information Flow Control | [VVoIP] |
| | FDP_IFF.1 | Simple Security Attributes | [VVoIP] |
| FIA: Identification and authentication | FIA_X509_EXT.1 | X.509 Certificate Validation | [APP] |
| | FIA_X509_EXT.2 | X.509 Certificate Authentication | [APP] |
| FMT: Security management | FMT_MEC_EXT.1 | Supported Configuration Mechanism | [APP] |

| Class Name | Component Identification | Component Name | Drawn From |
|----------------------------|--------------------------|--|---------------|
| | FMT_CFG_EXT.1 | Secure by Default Configuration | [APP] |
| | FMT_SMF.1 | Specification of Management Functions | [APP] |
| | FMT_SMF.1/VVoIP | Specification of Management Functions (VVoIP Communications) | [VVoIP] |
| FPR: Privacy | FPR_ANO_EXT.1 | User Consent for Transmission of Personally Identifiable Information | [App] |
| FPT: Protection of the TSF | FPT_API_EXT.1 | Use of Supported Services and APIs | [App] |
| | FPT_AEX_EXT.1 | Anti-Exploitation Capabilities | [App] |
| | FPT_TUD_EXT.1 | Integrity for Installation and Update | [App] |
| | FPT_TUD_EXT.2 | Integrity for Installation and Update | [App] |
| | FPT_LIB_EXT.1 | FPT_LIB_EXT.1 Use of Third Party Libraries | [App] |
| | FPT_IDV_EXT.1 | Software Identification and Versions | [App] |
| FTA: TOE Access | FTA_SSL.3/Media | Media TSF-Initiated Termination (Media Channel) | [VVoIP] |
| FTP: Trusted path/channels | FTP_DIT_EXT.1 | Protection of Data in Transit | [App] [VVoIP] |
| | FTP_ITC.1/Control | Control Inter-TSF Trusted Channel (Signaling Channel) | [VVoIP] |
| | FTP_ITC.1/Media | Media Inter-TSF Trusted Channel (Media Channel) | [VVoIP] |

5.2.1 Class: Communications (FCO)

5.2.1.1 FCO_VOC_EXT.1 – Fixed-Rate Vocoder

FCO_VOC_EXT.1.1 The TSF shall transmit voice media using a constant bit rate voice vocoder.

5.2.2 Class: Cryptographic Support (FCS)

5.3.2.1 FCS_CKM_EXT.1 – Cryptographic Key Generation Services

FCS_CKM_EXT.1.1 The application shall [implement asymmetric key generation].

5.3.2.2 FCS_CKM.1/KeyGen – Cryptographic Asymmetric Key Generation

FCS_CKM.1.1/KeyGen The application shall [implement functionality] to generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm [

- [RSA schemes] using cryptographic key sizes of **[2048-bit or greater]** that meet the following: **FIPS PUB 186-4, “Digital Signature Standard (DSS), Appendix B.3”**;

- **[ECC schemes] using [“NIST curves” P-256, P-384 and [P-521]] that meet the following: [FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4]**

].

5.3.2.3 FCS_CKM.2 – Cryptographic Key Establishment

FCS_CKM.2.1 The application shall [implement functionality] to perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [

- **[Elliptic curve-based key establishment schemes] that meets the following: [NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”]**

].

5.3.2.4 FCS_COP.1/Encrypt – Cryptographic Operation – Encryption/Decryption

FCS_COP.1.1/Encrypt The application shall perform encryption/decryption in accordance with a specified cryptographic algorithm [

- AES-CBC (as defined in NIST SP 800-38A) mode,
- AES-GCM (as defined in NIST SP 800-38D) mode,

] and cryptographic key sizes [128-bit, 256-bit].

Application Note: This requirement has applied NIAP TD-0598

5.3.2.5 FCS_COP.1/Hash – Cryptographic Operation – Hashing

FCS_COP.1.1/Hash The **application** shall perform *cryptographic hashing* services in accordance with a specified cryptographic algorithm

- [SHA-1, SHA-256, SHA-384]

and message digest sizes

- [160, 256, 384]

bits that meet the following: FIPS Pub 180-4.

5.3.2.6 FCS_COP.1/SigGen – Cryptographic Operation – Signing

FCS_COP.1.1/SigGen The **application** shall perform *cryptographic signature services (generation and verification)* in accordance with a specified cryptographic algorithm [

- **[RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 4]**

].

5.3.2.7 FCS_COP.1/KeyHash – Cryptographic Operation – Keyed-Hash Message Authentication

FCS_COP.1.1/KeyHash The **application** shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm

- HMAC-SHA-256

and

- [SHA-1, SHA-384]

with key sizes [160, 256, 384 used in HMAC] and message digest sizes 256 and [160, 384] bits that meet the following: FIPS Pub 198-1 *The Keyed-Hash Message Authentication Code* and FIPS Pub 180-4 *Secure Hash Standard*.

5.3.2.8 FCS_COP.1/SRTP – Cryptographic Operation – Encryption/Decryption for SRTP

FCS_COP.1.1/SRTP The TSF shall perform *[encryption/decryption to support SDES-SRTP]* in accordance with a specified cryptographic algorithm [AES-CTR (as defined in NIST SP 800-38A), AES-GCM (as defined in NIST SP 800-38D)] and cryptographic key sizes [128-bit, 256-bit].

5.3.2.9 FCS_RBG_EXT.1 – Random Bit Generation Services

FCS_RBG_EXT.1.1 The application shall [invoke platform-provided DRBG functionality] for its cryptographic operations.

5.3.2.10 FCS_STO_EXT.1 – Storage of Credentials

FCS_STO_EXT.1.1 The application shall [invoke the functionality provided by the platform to securely store [private keys, passwords]] to non-volatile memory.

5.3.2.11 FCS_SRTP_EXT.1 – Secure Real-Time Transport Protocol

FCS_SRTP_EXT.1.1 The TSF shall implement the Secure Real-Time Transport Protocol (SRTP) that complies with RFC 3711, and use Security Descriptions for Media Streams (SDES) in compliance with RFC 4568 to provide key information for the SRTP connection.

FCS_SRTP_EXT.1.2 The TSF shall implement SDES-SRTP supporting the following ciphersuites [

- AEAD_AES_256_GCM, in accordance with RFC 7714].

FCS_SRTP_EXT.1.3 The TSF shall ensure the SRTP NULL algorithm can be disabled.

FCS_SRTP_EXT.1.4 The TSF shall allow the SRTP ports to be used for SRTP communications to be specified by an Authorized Administrator.

5.3.2.12 FCS_TLS_EXT.1 – TLS Protocol

FCS_TLS_EXT.1.1 The product shall implement [

- TLS as a client

].

5.3.2.13 FCS_TLSC_EXT.1 – TLS Client Protocol

FCS_TLSC_EXT.1.1 The product shall implement TLS 1.2 (RFC 5246) and [no earlier TLS versions] as a client that supports the cipher suites [

- TLS ECDHE RSA WITH AES 128 GCM SHA256 as defined in RFC 5289,
- TLS ECDHE RSA WITH AES 256 GCM SHA384 as defined in RFC 5289,
- TLS ECDHE RSA WITH AES 128 CBC SHA256 as defined in RFC 5289,
- TLS ECDHE RSA WITH AES 256 CBC SHA384 as defined in RFC 5289]

and also supports functionality for [session renegotiation].

FCS_TLSC_EXT.1.2 The product shall verify that the presented identifier matches the reference identifier according to RFC 6125.

FCS_TLSC_EXT.1.3 The product shall not establish a trusted channel if the server certificate is invalid [with no exceptions].

5.3.2.14 FCS_TLSC_EXT.2 – TLS Client Support for Mutual Authentication

FCS_TLSC_EXT.2.1 The product shall support mutual authentication using X.509v3 certificates.

5.3.2.15 FCS_TLSC_EXT.4 – TLS Client Support for Renegotiation

FCS_TLSC_EXT.4.1 The product shall support secure renegotiation through use of the “renegotiation_info” TLS extension in accordance with RFC 5746.

5.3.2.16 FCS_TLSC_EXT.5 – TLS Client Support for Supported Groups Extension

FCS_TLSC_EXT.5.1 The product shall present the Supported Groups Extension in the Client Hello with the supported groups [secp256r1, secp384r1, secp521r1].

5.3.3 Class: User Data Protection (FDP)

5.3.3.1 FDP_DEC_EXT.1 – Access to Platform Resources

FDP_DEC_EXT.1.1 The application shall restrict its access to [

- network connectivity,
- camera,
- microphone,
- USB,
- Bluetooth

].

FDP_DEC_EXT.1.2 The application shall restrict its access to [

- address book,
- calendar,
- [file-system, photo library]

].

5.3.3.2 FDP_NET_EXT.1 – Network Communications

FDP_NET_EXT.1.1 The application shall restrict network communication to [

- user-initiated communication for [Voice/Video calls (SIP over TLS,SRTP)],
- respond to [Voice/Video calls (SIP over TLS,SRTP)]

].

5.3.3.3 FDP_DAR_EXT.1 – Encryption Of Sensitive Application Data

FDP_DAR_EXT.1.1 The application shall [protect sensitive data in accordance with FCS_STO_EXT.1] in non-volatile memory.

5.3.3.4 FDP_IFC.1 – Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the *[media transmission policy]* on *[voice/video media transmitted by the TOE]*.

5.3.3.5 FDP_IFF.1 – Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the *[media transmission policy]* based on the following types of subject and information security attributes: *[TOE hook state, VVoIP call connection status, and VVoIP call control server status]*.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- *The TOE is **[registered with a VVoIP call control server]**,*
- *A call has been established with a telephony device (VVoIP endpoint),*
- *The TOE is in the off-hook state,*
- *The TOE is not in the mute state,*
- ***[The TOE is not in the hold state]**.*

].

FDP_IFF.1.3 The TSF shall enforce *[no additional information flow control policy rules]*.

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: *[no additional rules]*.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: *[all TCP and UDP ports used by the TOE are closed when not in active use]*.

5.3.4 Class: Identification and Authentication (FIA)

5.3.4.1 FIA_X509_EXT.1 – X.509 Certificate Validation

FIA_X509_EXT.1.1 The application shall [invoke platform-provided functionality] to validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.
- The application shall validate a certificate path by ensuring the presence of the basicConstraints extension, that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met.
- The application shall validate that any CA certificate includes caSigning purpose in the key usage field.
- The application shall validate the revocation status of the certificate using [OCSP as specified in RFC 6960, CRL as specified in RFC 5759].
- The application shall validate the extendedKeyUsage (EKU) field according to the following rules:
 - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
 - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the EKU field.

- Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the EKU field.
- S/MIME certificates presented for email encryption and signature shall have the Email Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) in the EKU field.
- OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the EKU field.
- Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the EKU field.

Application Note: This requirement has applied NIAP TD-0587

FIA_X509_EXT.1.2 The application shall treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.

5.3.4.2 FIA_X509_EXT.2 – X.509 Certificate Authentication

FIA_X509_EXT.2.1 The application shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [TLS].

FIA_X509_EXT.2.2 When the application cannot establish a connection to determine the validity of a certificate, the application shall [accept the certificate].

5.3.5 Class: Security Management (FMT)

5.3.5.1 FMT_MEC_EXT.1 – Supported Configuration Mechanism

FMT_MEC_EXT.1.1 The application shall [invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.]

Application Note: This requirement has applied NIAP TD-0437

5.3.5.2 FMT_CFG_EXT.1 – Secure by Default Configuration

FMT_CFG_EXT.1.1 The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials.

FMT_CFG_EXT.1.2 The application shall be configured by default with file permissions which protect the application binaries and data files from modification by normal unprivileged users.

5.3.5.3 FMT_SMF.1 – Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions [no management functions].

5.3.5.4 FMT_SMF.1/VVoIP – Specification of Management Functions (VVoIP Communications)

FMT_SMF.1.1/VVoIP The TSF shall be capable of performing the following management functions: [

- Ability to [register the TOE to an ESC [manually]];
- [
- Ability to configure the termination period for idle calls].

5.3.6 Class: Privacy (FPR)

5.3.6.1 FPR_ANO_EXT.1 – User Consent for Transmission of Personally Identifiable Information

FPR_ANO_EXT.1.1 The application shall [not transmit PII over a network].

5.3.7 Class: Protection of the TSF (FPT)

5.3.7.1 FPT_API_EXT.1 – Use of Supported Services and APIs

FPT_API_EXT.1.1 The application shall use only documented platform APIs.

5.3.7.2 FPT_AEX_EXT.1 – Anti-Exploitation Capabilities

FPT_AEX_EXT.1.1 The application shall not request to map memory at an explicit address except for [*no exceptions*].

FPT_AEX_EXT.1.2 The application shall [not allocate any memory region with both write and execute permissions].

FPT_AEX_EXT.1.3 The application shall be compatible with security features provided by the platform vendor.

FPT_AEX_EXT.1.4 The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.

FPT_AEX_EXT.1.5 The application shall be built with stack-based buffer overflow protection enabled.

5.3.7.3 FPT_TUD_EXT.1 – Integrity for Installation and Update

FPT_TUD_EXT.1.1 The application shall [leverage the platform] to check for updates and patches to the application software.

FPT_TUD_EXT.1.2 The application shall [provide the ability] to query the current version of the application software.

FPT_TUD_EXT.1.3 The application shall not download, modify, replace or update its own binary code.

FPT_TUD_EXT.1.4 The application updates shall be digitally signed such that the application platform can cryptographically verify them prior to installation.

Application Note: This requirement has applied NIAP TD-0561

FPT_TUD_EXT.1.5 The application is distributed [as an additional software package to the platform OS].

5.3.7.4 FPT_TUD_EXT.2 – Integrity for Installation and Update

FPT_TUD_EXT.2.1 The application shall be distributed using the format of the platform-supported package manager.

FPT_TUD_EXT.2.2 The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events.

FPT_TUD_EXT.2.3 The application installation package shall be digitally signed such that its platform can cryptographically verify them prior to installation.

Application Note: *This requirement has applied NIAP TD-0561.*

5.3.7.5 FPT_LIB_EXT.1 – Use of Third Party Libraries

FPT_LIB_EXT.1.1 The application shall be packaged with only [*list of third-party libraries in table 13*].

Table 13. Third-Party Libraries

| Third-Party Libraries | Third-Party Libraries |
|-----------------------|-----------------------|
| angle | libusb |
| apr | libvorbis |

| Third-Party Libraries | Third-Party Libraries |
|-----------------------|-----------------------|
| blink | libvpx |
| boost | libwebp |
| boringsssl | libxml |
| cef | libxslt |
| curl | open-ldap |
| cyrus-sasl | opencore-amr |
| direct3d | openjpeg |
| expat | openssl |
| flutter | opus |
| free-type | ots |
| glew | pcre |
| glib | pdfium |
| gloox | poco |
| gsoap | protobuf |
| gstreamer | rapidxml |
| hunspell | re2 |
| icu | sipcc |
| jansson | skia |
| json-c | speexdsp |
| json-cpp | sql-cipher |
| kerberos | sqlite |
| leveldb | tidy |
| libcxx | tiny-xml |
| libflac | udt |
| libjpeg | v8 |
| libjpeg-turbo | visual-studio-runtime |
| libphonenumber | websocketpp |
| libpng | xmlrpc-c |
| libsrt | zlib |

5.3.7.6 FPT_IDV_EXT.1 Software Identification and Versions

FPT_IDV_EXT.1.1 The application shall be versioned with *[[sequence-based versioning control]]*.

5.3.8 Class: TOE Access (FTA)

5.3.8.1 FTA_SSL.3/Media – TSF-Initiated Termination (Media Channel)

FTA_SSL.3.1/Media The TSF shall terminate **voice/video transmission** after *[inactivity longer than [300 seconds, an administrator-configurable interval]]*.

5.3.9 Class: Trusted Path (FTP)

5.3.9.1 FTP_DIT_EXT.1 – Protection of Data in Transit

FTP_DIT_EXT.1.1 The application shall [

- encrypt all transmitted *[sensitive data]* with **TLS as defined in the TLS Package and [Secure Real-Time Transport Protocol (SRTP)]**,

] between itself and another trusted IT product.

5.3.9.2 FTP_ITC.1/Control – Inter-TSF Trusted Channel (Signaling Channel)

FTP_ITC.1.1/Control The TSF shall **be capable of using [Session Initiation Protocol (SIP)]** to provide a trusted communication channel between itself and a **VVoIP call control server** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.

FTP_ITC.1.2/Control The TSF shall permit *[the TSF, the VVoIP call control server]* to initiate communication via the trusted channel.

FTP_ITC.1.3/Control The TSF shall initiate communication via the trusted channel for *[establishment of call control]*.

5.3.9.3 FTP_ITC.1/Media – Inter-TSF Trusted Channel (Media Channel)

FTP_ITC.1.1/Media The TSF shall **be capable of using [SRTP]** to provide a trusted communication channel between itself and **another VVoIP endpoint or other telephony device** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.

FTP_ITC.1.2/Media The TSF shall permit *[the TSF, another VVoIP endpoint or other telephony device]* to initiate communication via the trusted channel.

FTP_ITC.1.3/Media The TSF shall initiate communication via the trusted channel for *[transmission of voice/video media]*.

5.4 Security Assurance Requirements

5.4.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from [APP] and [VVoIP] which are derived from [CC_PART3]. The assurance requirements are summarized in the table below.

Table 14. SAR Requirements

| Assurance Class | Components Description |
|--------------------------------|---|
| Security Target (ASE) | Conformance claims (ASE_CCL.1) |
| | Extended components definition (ASE_ECD.1) |
| | ST introduction (ASE_INT.1) |
| | Security objectives for the operational environment (ASE_OBJ.1) |
| | Security objectives (ASE_OBJ.2) |
| | Stated security requirements (ASE_REQ.1) |
| | Derived security requirements (ASE_REQ.2) |
| | Security Problem Definition (ASE_SPD.1) |
| | TOE summary specification (ASE_TSS.1) |
| Development (ADV) | Basic functional specification (ADV_FSP.1) |
| Guidance documents (AGD) | Operational user guidance (AGD_OPE.1) |
| | Preparative procedures (AGD_PRE.1) |
| Life cycle support (ALC) | Labeling of the TOE (ALC_CMC.1) |
| | TOE CM coverage (ALC_CMS.1) |
| | Timely Security Updates (ALC_TSU_EXT.1) |
| Tests (ATE) | Independent testing – conformance (ATE_IND.1) |
| Vulnerability assessment (AVA) | Vulnerability survey (AVA_VAN.1) |

5.4.2 SAR Rationale

The Security Assurance Requirements (SARs) in this Security Target represent the SARs identified in the [APP], [VVoIP], and [TLS]. As such, the [APP], [VVoIP], and [TLS] SAR rationale is deemed acceptable since the PP themselves have been validated.

5.5 Assurance Measures

The TOE satisfies the identified assurance requirements. This section identifies the Assurance Measures applied by Cisco to satisfy the assurance requirements. The table below lists the details.

Table 15. Assurance Measures

| Assurance Component | How Requirement Will Be Met |
|---------------------|--|
| ADV_FSP.1 | No additional “functional specification” documentation was provided by Cisco to satisfy the Evaluation Activities specified in the SD. |

| Assurance Component | How Requirement Will Be Met |
|------------------------|--|
| AGD_OPE.1 AGD_PRE.1 | Guidance must include a description of how the IT personnel verifies that the Operational Environment can fulfill its role for the security functionality. The documentation should be in an informal style and readable by the IT personnel. Guidance must be provided for every operational environment that the product supports as claimed in the ST. This guidance includes: <ul style="list-style-type: none"> • instructions to successfully install the TSF in that environment; and • instructions to manage the security of the TSF as a product and as a component of the larger operational environment; and • instructions to provide a protected administrative capability. Guidance pertaining to particular security functionality must also be provided. Cisco will provide the guidance documents with the ST. |
| ALC_CMC.1 ALC_CMS.1 | Cisco will identify the TOE such that it can be distinguished from other products or versions from the Cisco and can be easily specified when being procured by an end user. |
| ALC_TSU_EXT.1 | Cisco will provide a Security Vulnerability Policy. |
| ATE_IND.1 | Cisco will provide the TOE for testing. |
| AVA_VAN.1 | Cisco will provide the TOE for Vulnerability Analysis. |

6 TOE Summary Specification

6.1 TOE Security Functional Requirement Measures

The table below identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 16. How TOE SFRs Measures Are Met

| TOE SFRs | How the SFR is Met |
|-------------------|---|
| FCO_VOC_EXT.1 | <p>The Cisco Jabber TOE transmits voice media using a constant bitrate (CBR) vocoder which ensures packet length is the same. The constant bitrate voice codecs implemented by the TSF are: G.711A, G.711u, G.722, G.722.1 and G.729.</p> <ul style="list-style-type: none"> • G.711 - The most commonly supported codec, used over the public switched telephone network. • G.722 - A wideband codec that is always preferred by Cisco Unified Communications Manager over G.711, unless G.722 is disabled. Audio codec often used in video conferences. • G.722.1 - A low-complexity wideband codec operating at 24 and 32 kb/s. The audio quality approaches that of G.722 while using at most half the bit rate. As it is optimized for both speech and music, G.722.1 has slightly lower speech quality than the speech-optimized iSAC codec. • G.729 - A Low-bit-rate codec with 8-kb/s compression that is typically used for calls across a WAN link because they use less bandwidth. |
| FCS_CKM_EXT.1 | <p>The TOE implements asymmetric cryptography in support of TLS</p> |
| FCS_CKM.1/KeyGen | <p>To support TLS the TOE implements a specified key generation algorithm to generate asymmetric cryptographic keys in accordance with RSA and ECC schemes that meet FIPS PUB 186-4. The key sizes are:</p> <ul style="list-style-type: none"> • RSA scheme: 2048-bit • ECC using NIST curve of P-256, P-384, and P-521 |
| FCS_CKM.2 | <p>To support TLS the TOE implements the following algorithms to perform key establishment:</p> <ul style="list-style-type: none"> • ECC key establishment schemes that meet SP800-56A. |
| FCS_COP.1/Encrypt | <p>The TOE provides symmetric encryption and decryption capabilities using AES as specified in ISO 18033-3 supporting the following modes:</p> <ul style="list-style-type: none"> ○ CBC mode as specified in ISO 10116. ○ GCM mode as specified in ISO 19772. <p>The TOE uses AES in the following protocol:</p> <ul style="list-style-type: none"> ○ TLS: CBC mode with key size of 128 and 256 bits. GCM mode with key sizes of 128 and 256 bits. |
| FCS_COP.1/Hash | <p>The TOE provides cryptographic hashing services using SHA-1, SHA-256, and SHA-384 as specified in FIPS Pub 180-3 “Secure Hash Standard.”</p> <p>SHA-256 and SHA-384 are used in TLS to validate server certificates on establishing TLS connections. SHA-256 and SHA-384 are used when the TOE generates asymmetric keys for Elliptic curve-based key establishment. SHA-1 is used with SRTP.</p> |

| TOE SFRs | How the SFR is Met |
|-------------------|--|
| | The hashing is used to support trusted updates where the TOE software is digitally signed using RSA 2048-bit key cryptography and SHA256 hashing. |
| FCS_COP.1/SigGen | The TOE provides cryptographic signature services using RSA Digital Signature Algorithm with key size of 2048. |
| FCS_COP.1/KeyHash | The TOE provides keyed-hashing message authentication services using HMAC-SHA-1(key size – 160 bits, block size 512 bits), HMAC-SHA-256 (key size – 256 bits, block size 512 bits), and HMAC-SHA-384 (key size – 384 bits, block size 1024 bits). |
| FCS_COP.1/SRTP | For the STRP protocol, the TOE implements AES in CTR mode with a key size of 128 bits and GCM mode with a key size of 128 or 256 bits. |
| FCS_RBG_EXT.1 | <p>The TOE invokes the BCryptGenRandom API on the platform when needed to generate a cryptographic key. This applies to the following SFRs:</p> <p>FCS_CKM.1/KeyGen – Cryptographic Asymmetric Key Generation FCS_CKM.2 – Cryptographic Key Establishment FCS_SRTP_EXT.1 – Secure Real-Time Transport Protocol</p> |
| FCS_STO_EXT.1 | <p>The Cisco Jabber TOE leverages the platform for securely storing persistent credentials. The TOE stores the following to the Windows Credential Manager:</p> <ul style="list-style-type: none"> • The private key used for X.509 certificate generation and peer authentication • User password (secret) |
| FCS_SRTP_EXT.1 | <p>The TOE implements secure RTP (SRTP) as defined in RFC 3711 to provide encryption and authentication of audio and video data streams between itself and a VVoIP endpoint. The TOE uses AES encryption/decryption supporting the following ciphersuites:</p> <ul style="list-style-type: none"> • AEAD_AES_256_GCM <p>For incoming and outgoing calls, SRTP keys are exchanged as defined in section 4 of RFC 4568. The TOE uses the Session Description Protocol (SDP) within SIP signaling messages as the “inline” parameter within SDP packets. SRTP key exchange is accomplished through the "crypto" attribute (a=crypto) under the particular media type (m=video or m=audio) within the SDP. The format of the "crypto" attribute is shown below.</p> <p style="text-align: center;">a=crypto:<tag> <crypto-suite> <key-params> [<session-params>]</p> <p>The tag field is a decimal number used to uniquely distinguish multiple crypto attributes from each other. The crypto-suite field contains the cipher and message authentication algorithms for the particular crypto attribute. The key-params field itself has the format shown below.</p> <p style="text-align: center;">key-params = <key-method> ":" <key-info></p> <p>The key-method field indicates the method by which keying material is exchanged and ‘inline’ indicates the keying information is contained within the SDP. An example of the use of SDP for SRTP is shown below:</p> <pre style="text-align: center;">m=video 16386 RTP/SAVP 112 c=IN IP4 14.50.248.31 a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:d0RmdmcmVCspeEc3QGZiNWpVLFJhQX1cfHAwJSoj 2^20 1:32</pre> |

| TOE SFRs | How the SFR is Met | | | | | | | | | |
|----------------------|---|--|-------------|-------------|------|--------------|----------------------|----------------------|------|--|
| | <p>Since keying material is sent within SIP signaling, encryption of the SIP signaling is required to secure the key exchange. The TOE implements TLS to protect the SRTP key exchange between itself and the CUCM server. The CUCM SIP Server is responsible for the configuration of the policy regarding which ciphers are allowed. The TOE cannot override this configuration. The evaluated configuration requires the administrator of the CUCM SIP Server to configure only 'secure/encrypted' calls. By doing so attempts to call using SRTP NULL encryption fail.</p> | | | | | | | | | |
| FCS_TLSC_EXT.1 | <p>The Cisco Jabber TOE implements TLS 1.2 with the following ciphersuites:</p> <p>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384</p> | | | | | | | | | |
| FCS_TLSC_EXT.5 | <p>The Cisco Jabber TOE implements secp256r1, secp384r1, secp521r1 elliptic curve extensions in the supported groups extension of the Client Hello packet. This is the behaviour by default and is not configurable.</p> | | | | | | | | | |
| FDP_DEC_EXT.1 | <p>The Cisco Jabber TOE restricts access to the following network connectivity resources: camera, microphone, USB, and Bluetooth. To function as a VVoIP product, access to network connectivity, the camera, and microphone resources are required.</p> <p>In addition, the TOE can access Bluetooth or USB hardware resources to control Bluetooth or USB audio devices.</p> <p>The TOE restricts its access to the following repositories:</p> <ul style="list-style-type: none"> ○ Address book and calendar – Needed to import contacts and for calling VVoIP users. ○ File-system - To import contacts, access to the file system is needed. ○ Photo Library - Users may import a photo from the photo library to be used on VVoIP calls. <p>Note: While Jabber is capable of integration with Microsoft Outlook, IBM Lotus Notes and Google Calendar, only the integration with Microsoft Outlook is evaluated and the AGD only details the configuration for the Microsoft Outlook.</p> | | | | | | | | | |
| FDP_NET_EXT.1 | <p>The Cisco Jabber TOE limits network communication to the following:</p> <ul style="list-style-type: none"> ○ Initiation: Jabber allows initiation of Voice/Video (SIP over TLS/SRTP). ○ Jabber responds to: Voice/Video (SIP over TLS and SRTP communication initiated by a remote VoIP application via the ESC). <p>Port/Protocol usage is listed in the table below:</p> <table border="1" data-bbox="461 1398 1451 1654"> <thead> <tr> <th data-bbox="461 1398 802 1446">Port(s)</th> <th data-bbox="802 1398 1149 1446">Protocol(s)</th> <th data-bbox="1149 1398 1451 1446">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="461 1446 802 1495">5061</td> <td data-bbox="802 1446 1149 1495">SIP over TLS</td> <td data-bbox="1149 1446 1451 1495">Secure SIP signaling</td> </tr> <tr> <td data-bbox="461 1495 802 1654">16384 to 32766 (UDP)</td> <td data-bbox="802 1495 1149 1654">SRTP</td> <td data-bbox="1149 1495 1451 1654">Cisco Unified Communications Manager media port range used for audio, video, and BFCP video desktop share.</td> </tr> </tbody> </table> | Port(s) | Protocol(s) | Description | 5061 | SIP over TLS | Secure SIP signaling | 16384 to 32766 (UDP) | SRTP | Cisco Unified Communications Manager media port range used for audio, video, and BFCP video desktop share. |
| Port(s) | Protocol(s) | Description | | | | | | | | |
| 5061 | SIP over TLS | Secure SIP signaling | | | | | | | | |
| 16384 to 32766 (UDP) | SRTP | Cisco Unified Communications Manager media port range used for audio, video, and BFCP video desktop share. | | | | | | | | |
| FDP_DAR_EXT.1 | <p>Sensitive data in the TOE is defined as:</p> <ul style="list-style-type: none"> • The private key used for X.509 certificate generation and peer authentication • User password (secret) <p>Each is protected in accordance with FCS_STO.EXT.1</p> | | | | | | | | | |

| TOE SFRs | How the SFR is Met |
|--|---|
| | <p>The Cisco Jabber TOE leverages the platform for securely storing persistent credentials. Specifically the TOE stores them to the Windows Credential Manager.</p> |
| FDP_IFC.1 | <p>The TOE enforces a media transmission policy that ensures media data is not transmitted unless it is in a streaming media state as defined in the rules for FDP_IFF.1</p> |
| FDP_IFF.1 | <p>The TOE enforces a media transmission policy that ensures user voice and video data is not transmitted until the following is met:</p> <ul style="list-style-type: none"> • The TOE is registered with the ESC • A call has been established with a telephony device (VVoIP endpoint), • The TOE is in the off-hook state, • The TOE is not in the mute state, • The TOE is not in the hold state <p>When a call is placed on voice mute (silence), the voice steam is not stopped, but voice data from the microphone is no longer being sent. Silence or comfort noise packets are sent depending on the configuration settings by CUCM SIP Server. When on mute, the audio component is no longer transmitting a signal.</p> <p>Hold always results in the existing SRTP streams being stopped and new SRTP streams (with new keys) being negotiated over SIP/SDP with the Music on Hold service.</p> |
| FIA_X509_EXT.1 FIA_X509_EXT.2 FCS_TLSC_EXT.2 | <p>The Cisco Jabber TOE invokes platform functionality to perform the following certificate validation:</p> <ul style="list-style-type: none"> • Certificate validation and certificate path validation according to RFC 5280. • The certificate path must terminate with a trusted CA certificate. • All CA certificates must have the basicConstraints extension present and be of type CA=TRUE. • The certificate must not be revoked. Revocation is validated via the client device platform by OCSF and CRL revocation status check. • The certificate must not be expired. • The extendedKeyUsage field must be valid based on the following rules: <ul style="list-style-type: none"> ○ Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field. ○ Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field. ○ Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field. ○ S/MIME certificates presented for email encryption and signature shall have the Email Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) in the extendedKeyUsage field. ○ OCSF certificates presented for OCSF responses shall have the OCSF Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field. ○ Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the extendedKeyUsage field <p>The Cisco Jabber TOE compares the FQDN of the server it is establishing connectivity with against the Subject Alternate Name-dnsName attributes in the certificate. If Jabber determines there is a mismatch, it will not establish the TLS trusted channel. This applies to all TLS connections.</p> <p>The TOE does not support the use of wildcards within certificates and does not support certificate pinning.</p> <p>The TOE relies upon the client device platform to verify the certificate at the point in time when it receives the server certificate as part of the process of establishing a secure connection to any server. If</p> |

| TOE SFRs | How the SFR is Met |
|-----------------|---|
| | <p>the TOE platform is unable to connect to the OCSP responder for example due to a network error, the TOE will allow the certificate to be accepted.</p> <p>To obtain a X.509 certificate, the Cisco Jabber TOE must securely enroll in the Certificate Authority Proxy Function (CAPF) as instructed in the AGD. CAPF runs on the Cisco Unified Communications Manager and provides the TOE with X.509 certificates. The CAPF process also determines the certificate the TOE will use to establish a TLS connection. TLS mutual authentication is supported for the SIP connection between the TOE and CUCM Server.</p> |
| FMT_MEC_EXT.1 | The Cisco Jabber TOE reads its configuration stored remotely on the SIP Server |
| FMT_CFG_EXT.1 | The Cisco Jabber TOE is not installed with any preset default credentials. Users can only access files that are associated to the installation that user performed. |
| FMT_SMF.1 | There are no security management functions performed by the Cisco Jabber TOE. The TSF automatically operates in a manner that meets the SFRs by default. |
| FMT_SMF.1/VVoIP | The TSF provides the ability to register the TOE to an Enterprise Session Controller (ESC) and specifying the termination period for idle calls. See additional detail in FTA_SSL.3/Media. |
| FPR_ANO_EXT.1 | The Cisco Jabber TOE does not transmit PII |
| FPT_API_EXT.1 | <p>The Cisco Jabber TOE uses the following Windows APIs:</p> <ul style="list-style-type: none"> wevtapi.dll ESENT.dll UIAutomationCore.DLL WKSCLI.DLL dxcore.dll PROPSYS.dll dxgi.dll dxva2.dll d3d11.dll d3d9.dll dwmapi.dll CRYPTUI.dll USP10.dll WINMMBASE.dll WINMM.dll DWrite.dll UxTheme.dll OLEACC.dll gdiplus.dll COMCTL32.dll credui.dll atlthunk.dll MSIMG32.dll WINHTTP.dll DNSAPI.dll dhcpcsvc.DLL iertutil.dll urlmon.dll SAMCLI.DLL NTASN1.dll WININET.dll ncrypt.dll NETUTILS.DLL NETAPI32.dll Secur32.dll USERENV.dll WTSAPI32.dll IPHLPAPI.DLL |

| TOE SFRs | How the SFR is Met |
|---------------|--|
| | VERSION.dll CRYPTBASE.dll SspiCli.dll IMM32.dll bcrypt.dll NSI.dll SHLWAPI.dll win32u.dll powrprof.dll shcore.dll GDI32.dll WS2_32.dll cryptsp.dll OLEAUT32.dll gdi32full.dll RPCRT4.dll cfgmgr32.dll WLDAP32.dll bcryptPrimitives.dll appcore.dll COMDLG32.dll ole32.dll KERNELBASE.dll UMPDC.dll SHELL32.dll sechost.dll profapi.dll msvcp_win.dll ADVAPI32.dll WINTRUST.dll USER32.dll storage.dll CRYPT32.dll ucrtbase.dll combase.dll MSASN1.dll KERNEL32.DLL msvcrt.dll ntdll.dll HID.DLL d2d1.dll WINSPOOL.DRV |
| FPT_AEX_EXT.1 | The compiler flag used to enable ASLR when the Cisco Jabber TOE is compiled is /DYNAMICBASE. The compiler flag used to enable stack-based buffer overflow protection in the Cisco Jabber TOE is /GS. |
| FPT_IDV_EXT.1 | The Cisco Jabber TOE uses a sequence-based versioning control system. The application uses the “major. minor. maintenance. build” format for versioning control. For example: 14.0.4.56553. <ul style="list-style-type: none"> - Major (14 in the example above) designates a release where significant new features are added. - Minor (0 in the example above) designates a release where minor new features are added. - Maintenance Release (4 in the example above). - Build (56553 in the example above) are typically patches for vulnerabilities or bugs. |
| FPT_LIB_EXT.1 | The Cisco Jabber TOE uses the third-party libraries defined in table 13 |

| TOE SFRs | How the SFR is Met |
|---|--|
| FPT_TUD_EXT.1 FPT_TUD_EXT.2 ALC_TSU_EXT.1 | <p>The TOE has specific versions that can be queried by a user. A TOE update is not a patch applied to the existing TOE; it is a new version of the TOE. When TOE updates are made available by Cisco, an administrator can obtain and install the update. TOE software is digitally signed using RSA 2048-bit key and SHA256 hash, which is inline with the claims made for FCS_COP.1/Hash and FCS_COP.1/Sig-Gen. The platform performs verification and performs an install/upgrade/update if verification is successful. The authorized source for the digitally signed updates is "Cisco Systems, Inc". In a production environment, distribution to end users is typically achieved by use of a Mobile Device Management (MDM) solution. MDM solutions allow Administrators to deploy the TOE software in mass while maintaining control of software version, mode of operation, and feature selection.</p> <p>All Cisco communications relating to security issues are handled by the Cisco Product Security Incident Response Team (PSIRT). Cisco aims to provide fixes in 30 days, but depending on the timing, it may be greater than 30 days though not more than 60 days for most security issues. Fixes may be delayed longer for low-risk security issues. Updates are then made available at Cisco Software Central at: https://software.cisco.com.</p> <p>Customers can subscribe to the Cisco Notification Service to receive important information regarding product updates. Full information is provided in the Cisco Security Vulnerability Policy available at https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html</p> <p>Customers may securely report security issues to Cisco Support. For details on engaging Cisco Support, please reference Annex E: Obtaining Documentation and Submitting a Service Request.</p> |
| FTA_SSL.3/Media | <p>The Administrator can specify a remote call disconnect timer parameter in the jabber-config.xml file. If the "CommonCriteriaEndCallTimeout" parameter is specified, the administrator can set a value from 1 to 480 minutes. By default, Jabber will automatically terminate the voice/video media transmission to the remote peer if it determines it is no longer receiving SRTP/SDES traffic after 300 seconds (5 minutes) when operating in CC mode.</p> |
| FTP_DIT_EXT.1 | <p>The Cisco Jabber TOE uses TLS and SRTP to encrypt transmitted sensitive data.</p> |
| FTP_ITC.1/Control FTP_ITC.1/Media | <p>Each time the TOE initiates or receives a VVoIP call, TLS is used to protect the SIP session management communication between itself and the ESC. Communication between the TOE and the remote VVoIP endpoint is protected with SRTP.</p> |

7 Supplemental TOE Summary Specification Information

See table below for CAVP certificates.

Table 17. CAVP Certificates

| Platform/CPU | SFR | Algorithm | CAVP Certificate Number |
|--|-------------------|-------------|-------------------------|
| Windows 10 on Intel Core i5 (Tiger Lake) | FCS_CKM.1/KeyGen | RSA | A1420 |
| Windows 10 on Intel Core i5 (Tiger Lake) | FCS_CKM.2 | CVL-KAS-ECC | A1420 |
| Windows 10 on Intel Core i5 (Tiger Lake) | FCS_COP.1/Encrypt | CBC, GCM | A1420 |
| Windows 10 on Intel Core i5 (Tiger Lake) | FCS_COP.1/SRTP | CTR, GCM | A1420 |
| Windows 10 on Intel Core i5 (Tiger Lake) | FCS_COP.1/Hash | SHS | A1420 |
| Windows 10 on Intel Core i5 (Tiger Lake) | FCS_COP.1/SigGen | RSA | A1420 |
| Windows 10 on Intel Core i5 (Tiger Lake) | FCS_COP.1/KeyHash | HMAC | A1420 |

8 Annex A: References

The documentation listed below was used to prepare this ST.

Table 18. References

| Identifier | Description |
|------------|--|
| [CC_PART1] | Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-001 |
| [CC_PART2] | Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-002 |
| [CC_PART3] | Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-003 |
| [CEM] | Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-004 |
| [APP] | Protection Profile for Application Software, v1.3, March 1, 2019 |
| [VVoIP] | PP-Module for Voice and Video over IP (VVoIP), v1.0, October 28, 2020 |
| [TLS] | Functional Package for TLS, v1.1, March 1, 2019 |

9 Annex B: Acronyms

The following acronyms and terms are common and may be used in this Security Target.

Table 19. Acronyms

| Acronym/Term | Definition |
|--------------|--|
| AES | Advanced Encryption Standards |
| API | Application Programming Interface |
| CBR | Constant bitrate |
| CC | Common Criteria |
| CEM | Common Evaluation Methodology |
| CDP | Certificate Distribution Point |
| CM | Configuration Management |
| CRL | Certificate Revocation List |
| CUCM | Cisco Unified Communication Manager |
| DRBG | Deterministic Random Bit Generator |
| EC-DH | Elliptic Curve-Diffie-Hellman |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| ESC | Enterprise Session Controller |
| ESP | Encapsulating Security Payload |
| GCM | Galois Counter Mode |
| HMAC | Hash Message Authentication Code |
| IP | Internet Protocol |
| IT | Information Technology |
| OCSP | Online Certificate Status Protocol |
| OS | Operating System |
| PP | Protection Profile |
| PRF | Pseudo-Random Functions |
| RFC | Request For Comment |
| SAR | Security Assurance Requirement |
| SDES | Security Descriptions for Media Streams |

| | |
|--------|---|
| SDP | Session Description Protocol |
| SHS | Secure Hash Standard |
| SIP | Session Initiation Protocol |
| SRTP | Security Real-Time Transport Protocol |
| ST | Security Target |
| TCP | Transport Control Protocol |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TLS | Transport Layer Security |
| TOE | Target of Evaluation |
| TSC | TSF Scope of Control |
| TSF | TOE Security Function |
| TSP | TOE Security Policy |
| UCM | [Cisco] Unified Communications Manager |
| UDP | User datagram protocol |
| VoIP | Voice over IP |
| VVoIP | Voice and Video over IP |

10 Annex C: Terminology

The following terms are common and may be used in this Security Target.

Table 20. Terms

| Term | Definition |
|---|--|
| Authorized Administrator | Any user which has been assigned to a privilege level that is permitted to perform all TSF-related functions. |
| Certificate Authority Proxy Function (CAPF) | Process by which supported devices can request locally significant certificates by using Cisco Unified Communications Manager Administration. |
| CUCM | Cisco Unified Communications Manager (CUCM) serves as the software-based call-processing component of the Cisco Unified Communications family of products. The CUCM extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. CUCM is an Enterprise Session Controller. |
| Certificate Trust List (CTL) | A file signed by the Cisco Site Administrator Security Token (security token), that contains a list of certificates for servers that the phone is to trust. |
| CUCM (Call Manger) Cluster | A cluster refers to a CUCM Publisher (first CUCM server installed) and any associated Subscribers (CUCM servers installed after the Publisher and included in the Publishers servers list). For purposes of redundancy, Cisco recommends deployment of at least a Publisher an one subscriber, however from a functional standpoint, Jabber clients only register to a single server at a time. |
| CUCM (Call Manager) Node | A node refers to a member of a CUCM cluster. The term is used in reference to a publisher or associated Subscribers. |
| Enterprise Session Controller (ESC) | A VVoIP infrastructure device that is used to set up and tear down calls between VVoIP endpoints |
| Peer | Another VVoIP device also in communication with the CUCM that is capable of exchanging media packets with the TOE as part of an establishes media session. |
| Session Initiation Protocol (SIP) | A communications protocol defined by IETF that is used for creating, modifying, and terminating multimedia sessions with multiple participants. |
| Secure Real-Time Transport Protocol (SRTP) | A protocol that is used to provide multimedia (voice/video) streaming services with added security of encryption, message authentication and integrity, and replay protection. |
| SIP Server | The SIP Server (in this evaluation it is the Cisco Unified Communications Manager (CUCM) interacts with a VoIP client (TOE) and provides registrar and proxy capabilities required for call-session management as well as establishing, processing, and terminating VoIP calls. |
| User | Any entity (human user or external IT entity) outside the TOE that interacts with the TOE. |

11 Annex D: Differing SFR Naming Conventions

Note that iterations in [App] are identified with a number inside parentheses (e.g. "(1)") and iterations in [VVoIP] are identified by appending the SFR name with a slash and unique identifier suggesting the purpose of the iteration. This table serves to map on format to another.

Table 21. SFR Naming Map

| Component Name | Component Identification (Number) Format | Component Identification /Test Format |
|---|--|---------------------------------------|
| Cryptographic Operation - Encryption/Decryption | FCS_COP.1(1) | FCS_COP.1/Encrypt |
| Cryptographic Operation - Hashing | FCS_COP.1(2) | FCS_COP.1/Hash |
| Cryptographic Operation - Signing | FCS_COP.1(3) | FCS_COP.1/SigGen |
| Cryptographic Operation - Keyed-Hash Message Authentication | FCS_COP.1(4) | FCS_COP.1/KeyHash |
| SRTP Cryptographic Operation (Encryption/Decryption for SRTP) | FCS_COP.1(5) | FCS_COP.1/SRTP |
| Cryptographic Asymmetric Key Generation | FCS_CKM.1(1) | FCS_CKM.1/KeyGen |
| Password Conditioning | FCS_CKM.1(3) | FCS_CKM.1/Password |

12 Annex E: Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation at:

With CCO login: <http://www.cisco.com/en/US/partner/docs/general/whatsnew/whatsnew.html>

Without CCO login: <http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

You can access the most current Cisco documentation on the World Wide Web at the following sites:

<http://www.cisco.com>

Additionally, Cisco.com serves as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at any time, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.